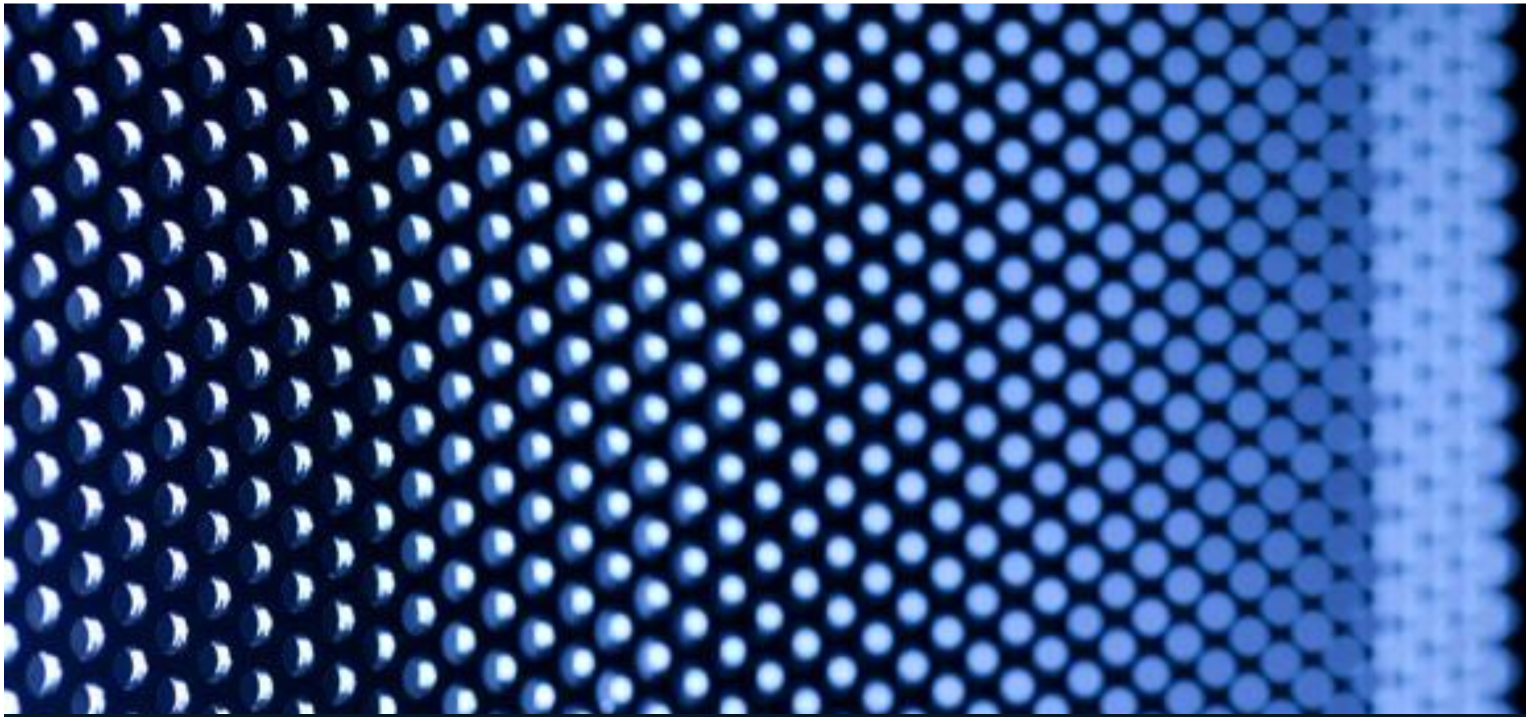


VERISIGN®

Considerations for Post Quantum DNSSEC

Andrew Fregly

March 9, 2022

Overview

The anticipated advent of Quantum Computers, capable of breaking current widely used public key cryptographic algorithms, is driving activities that will lead to development and adoption of new Post-Quantum Cryptographic algorithms within Internet security protocols.

This presentation covers some of Verisign's research and actions related to adoption of PQC algorithms for the DNSSEC use case.

Timeline for PQC DNSSEC

- Mosca's Model[1]: Exposure Time = (Migration Time + Shelf Time) - Threat Timeline
- DNSSEC Timeline Parameters:
  - Migration Time = Standardization Time + Transition Time
    - Standardization Time = conservatively 6 years given ~3 years for NIST Standards[2] and projecting an additional ~3 years for IETF RFCs
    - Transition Time: Experience with prior key and algorithm roll-overs indicates a 10-year transition period for PQC algorithms
  - Shelf Time: The "Shelf Time" of DNSSEC keys and signatures can be modeled as 0, because the keys are for authentication only (not confidentiality or non-repudiation)
  - Threat Timeline: Expert opinions range from 15 years to 50 years[1,15]
- Exposure = ((6+10) + 0) – 15 = 1 (one year exposure) to ((6+10) + 0) – 50 = -34 (34 year buffer before exposure)

Impetus For PQC-Related Action Now

- We are on the edge of a reasonable timeframe for DNSSEC adoption of the PQC algorithms from NIST's selection process
  - There is no certainty on when quantum computers will break current algorithms
  - We may not even know when this capability is achieved
- An earlier PQC solution for DNSSEC is desirable to address possible nearer-term availability of quantum computers capable of breaking current algorithms
- Preparation consisting of planning, testbeds, and standards activities can be done now with adoption performed on a timeline that is informed over time
  - Being prepared is not the same as adoption
  - Adoption without preparation is impossible
  - Preparation provides agility for adoption
- The DNS community should be engaged while PQC algorithms are actively being developed for other use cases (TLS, X.509 Certificates, ...)
  - It will be harder to influence PQC algorithms and implementations to address DNS's characteristics after they become mainstream
  - Algorithm diversity is a longstanding goal independent of the state of quantum computing -- it's helpful for DNSSEC to have alternatives in case of classical attacks on current algorithms

Some Observations Driving Our Activities

- Some of NIST's candidate algorithms[3,4,5] have resource requirements that make them less suitable for DNSSEC
  - Larger public keys
  - Larger signatures
  - CPU and memory requirements
- Even with EDNS(0)[6,7], UDP may be an unreliable transport for the large keys and signatures of PQC algorithms
- It is preferable to have small signatures regardless of key size
- Having all DNSKEY RRs returned in DNSKEY RRsets and all RRSIGs on an RRset returned in signed responses exacerbates the issues of large key and signature sizes

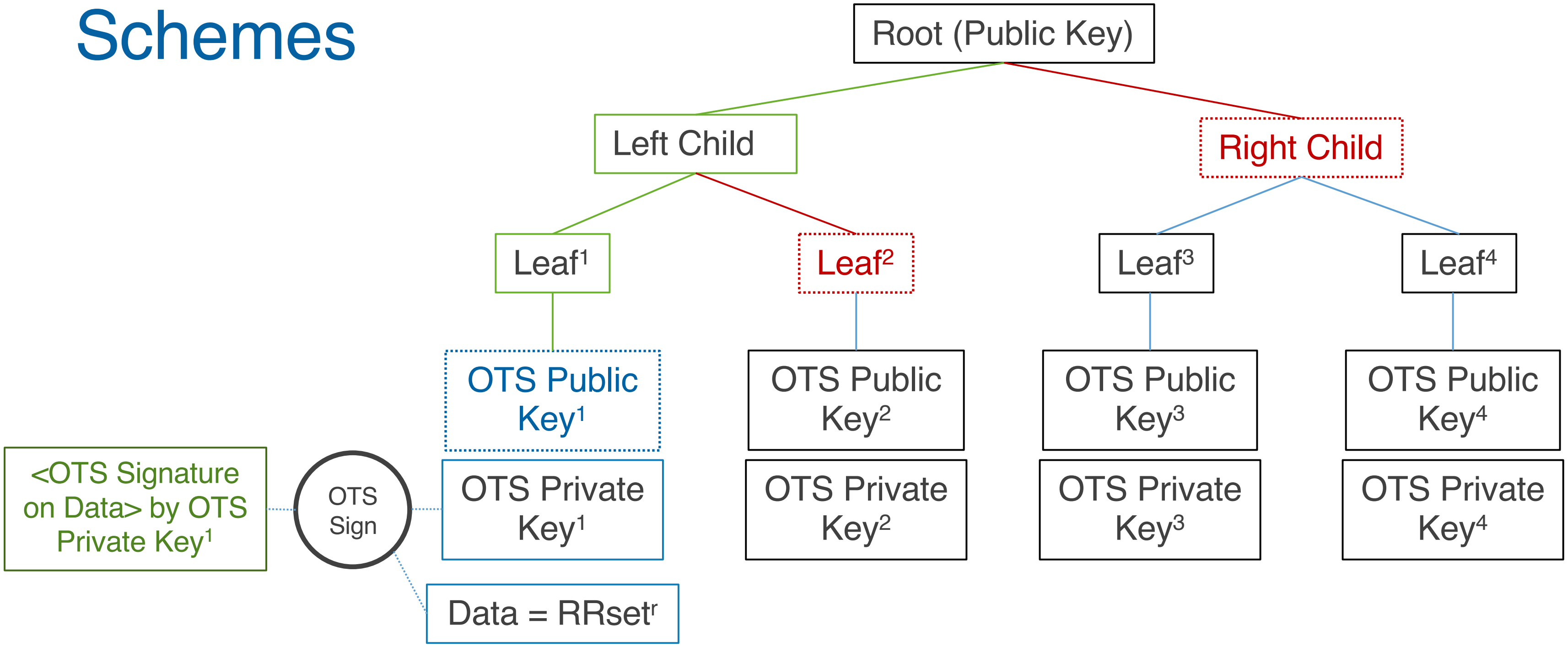
Hash-Based Signature Schemes as an Option for PQC Transition and Resilience

- Stateful Hash-Based Signature Schemes are public-key signature schemes first proposed by Ralph Merkle[8,9]
- Stateful Hash-Based Signature Schemes are a PQC solution that is recommended by NIST
  - Some hash functions are considered by NIST to be PQC[10]
  - Some Stateful Hash-Based Signature Schemes are NIST recommended PQC algorithms[8]
    - HSS/LMS[11]
    - XMSS/XMSS^{MT} [12]
- Design and cryptanalysis of hash functions over the last several decades has led to algorithms that have stood the test of time and which have wide adoption
  - SHA-2 algorithms[10]
  - SHAKE algorithms[10]
- Additional hash-based schemes for DNSSEC Consideration
  - SPHINCS+, a stateless hash-based signature scheme, is under consideration by the NIST PQC selection process[2]
  - “Synthesized” Public Keys based on Merkle trees as proposed by Burt Kaliski[13]

Merkle Trees and Stateful Hash-Based Signatures Schemes

- Scheme components include:
  - Merkle trees are binary trees where tree nodes are comprised of hashes of their children
  - Leaves are comprised of hashes of One Time Signature public keys
  - Per their name, private keys for OTS schemes can only be used once; multiple uses will reveal the private key
  - The root node of the Merkle tree serves as a public key for all signatures made by the OTS private keys corresponding to leaf nodes
  - Signatures are comprised of an OTS signature created with the OTS private key corresponding to an OTS public key, and an authentication path through the Merkle tree to use in verifying the OTS public key
  - Signature verification consists of deriving an OTS public key from the OTS signature, then walking the authentication path to verify the hash of the derived OTS public key is part of the Merkle tree whose root is the overall public key
- Given that OTS keys may only be used one time, a signer needs to keep track of signing state so as not to reuse OTS keys, thus the use of the term “Stateful Hash-Based Signature Schemes”

Signatures for Stateful Hash-Based Signatures Schemes



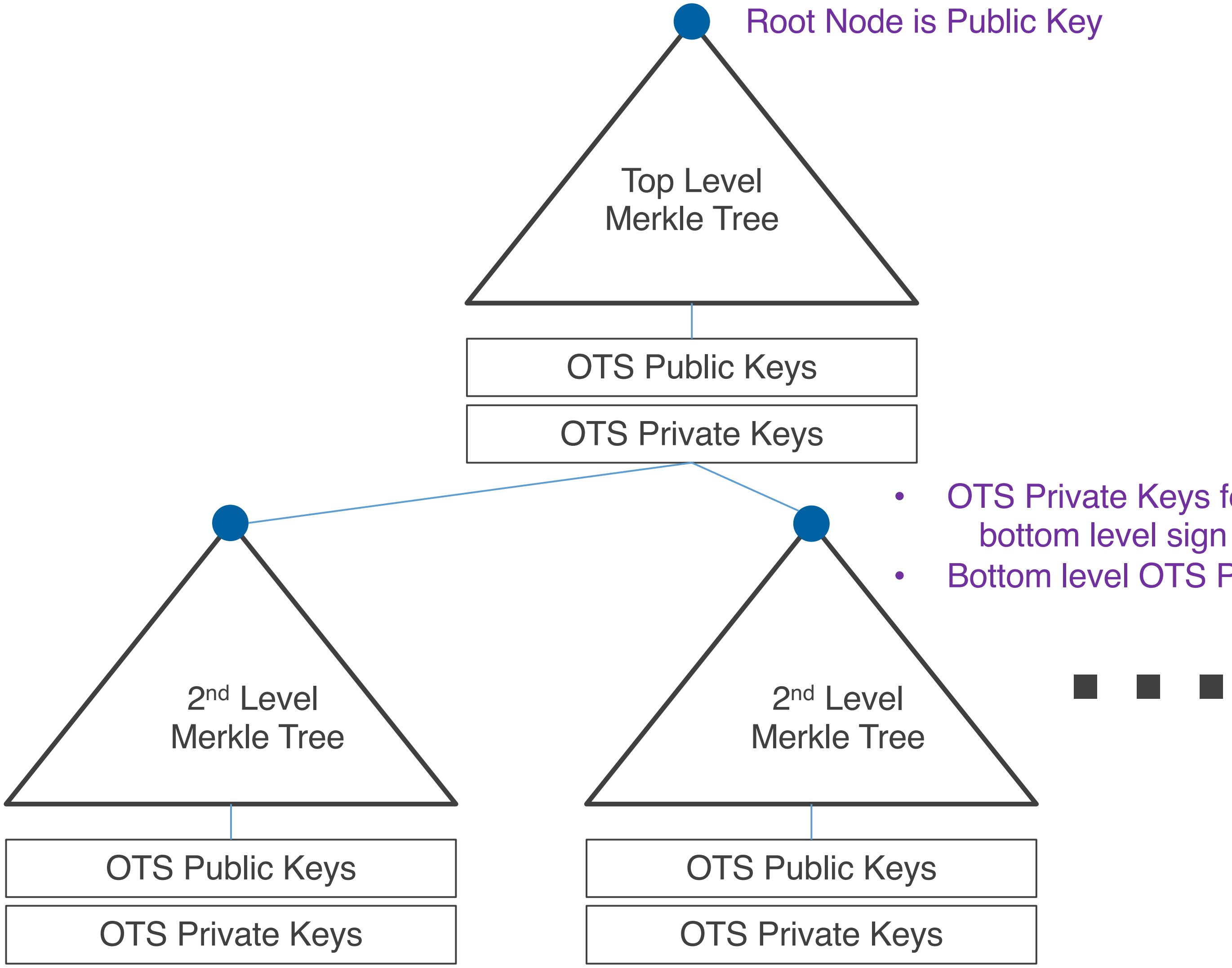
Signature Composition: <OTS Signature on Data><Authentication Path>

<Authentication Path>: consists of Merkle tree node hashes that are used as an input along with companion sibling nodes to calculate parent node hashes

Example for signature on RRset^r by OTS Public Key^1

> <OTS Signature on data> = Signature on data (RRset^r) created using OTS Private Key^1 corresponding to OTS Public Key^1
>
> <OTS Public Key> = OTS Public Key^1
>
> <Authentication Path> = Leaf^2 I Right Child

Hierarchical Tree Structures for Stateful Hash-Based Signature Schemes



Root Node is Public Key

- OTS Private Keys for levels above the bottom level sign roots of child trees
- Bottom level OTS Private Keys sign data

IETF Draft: Stateful Hash-Based Signatures for DNSSEC

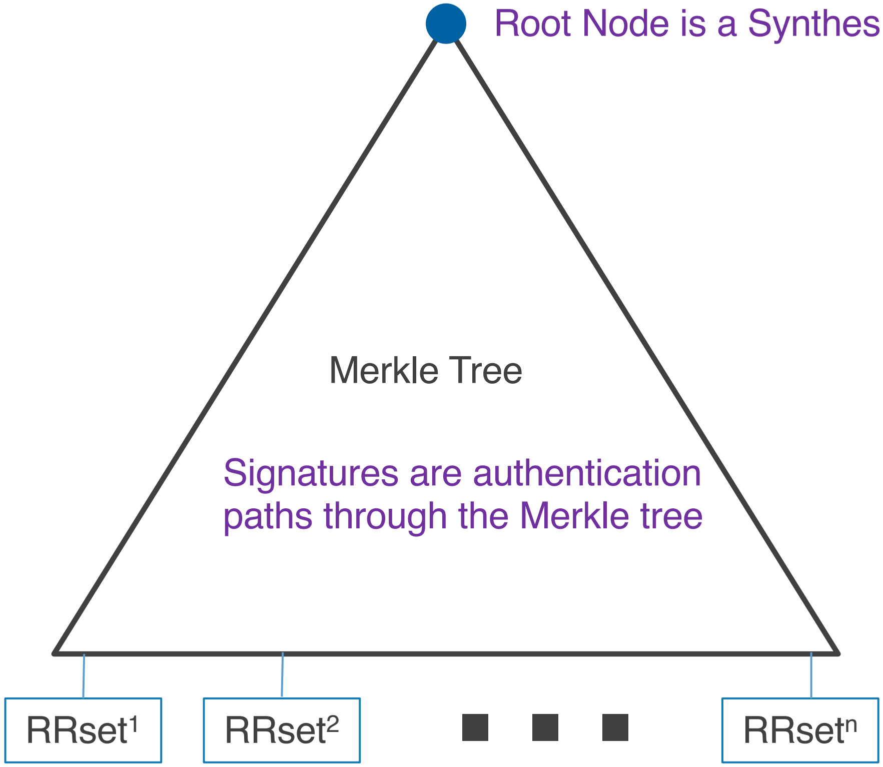
- Submitted draft "Stateful Hash-Based Signatures for DNSSEC"[14] to IETF
  - Specifies how HSS/LMS, XMSS, and XMSS^{MT} may be used in DNSSEC
  - Focused on representing keys and signatures as DNSKEY and RRSIG records
  - Touches on operational issues
- We are considering developing a draft that will dive deeper into operational issues

Implementation Considerations for Stateful Hash-Based Signatures for DNSSEC

- Interoperability Across Implementations
- Trade-offs of Hierarchical Trees
- Public Keys
- Operational Considerations

Synthesized Zone Signing Keys Using Merkle Trees[13]

Synthesized Zone Signing Keys[13] are an alternative hash-based approach for DNSSEC with shorter signatures than HBSS



Root Node is a Synthesized ZSK

Merkle Tree

Signatures are authentication paths through the Merkle tree

RRset^{1} RRset^{2} ■ ■ ■ RRset^{n}

Records signed by the Synthesized ZSK are comprised of RRsets. RRsets are inputs to hash calculation for the Merkle tree leaves.

Going Forward

- R&D: Algorithm characteristics; network and computing resource impact; test beds; operational experience; ecosystem readiness
- Planning: Collaborative activities; standards; transition
- Standards: IETF drafts for PQC algorithms for DNSSEC; operational guidance; NIST PQC evaluation
- Collaboration: PQC impact on DNSSEC operations; Resolver/Nameserver/Crypto Library support for PQC algorithms; legacy systems impact; DNSSEC over-the-wire analysis; test beds

References

1 - M. Mosca, M. Piani, "Quantum Threat Timeline Report 2020", 2020, https://globalriskinstitute.org/download/quantum-threat-timeline-report-2020/

2 - D. Moody, "NIST Status Update on the 3rd Round", "NIST 3rd PQC Standardization Conference", Jun 2021, https://csrc.nist.gov/CSRC/media/Presentations/status-update-on-the-3rd-round/images-media/session-1-moody-nist-round-3-update.pdf

3 - Open Quantum Safe, "Sig performance", Jan 2022, https://openquantumsafe.org/benchmarking/visualization/speed_sig.html

4 - Open Quantum Safe, "Sig memory consumption", Jan 2022, https://openquantumsafe.org/benchmarking/visualization/mem_sig.html

5 - D. Moody, "Round 2 of the NIST PQC "Competition" - What was NIST Thinking?", May 2019, https://csrc.nist.gov/CSRC/media/Presentations/Round-2-of-the-NIST-PQC-Competition-What-was-NIST/images-media/pqcrypto-may2019-moody.pdf

6 – O. Surý, "DNS Flag Day 2020", September 2020, https://www.isc.org/blogs/dns-flag-day-2020-2.

7 - K. Fujiwara, P. Vixie, "Fragmentation Avoidance in DNS", Work in Progress, Internet-Draft, draft-ietf-dnsop-avoid-fragmentation-05, June 2021, https://datatracker.ietf.org/doc/draft-ietf-dnsop-avoid-fragmentation/

8 – R. C. Merkle, “Secrecy, authentication, and public key systems”, UMI Research Press, 1982, ISBN 0-8357-1384-9

9 – R. C. Merkle, "A Digital Signature Based on a Conventional Encryption Function”, Advances in Cryptology — CRYPTO '87. Lecture Notes in Computer Science. Vol. 293, doi:10.1007/3-540-48184-2_32, ISBN 978-3-540-18796-7.

10 - National Institute of Standards and Technology (NIST), "SP 800-208 Recommendation for Stateful Hash-Based Signature Schemes", October 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf

11 – D. McGrew, M. Curcio, S. Fluhrer, "Leighton-Micali Hash-Based Signatures", RFC 8554, DOI 10.17487/RFC8554, April 2019, https://www.rfc-editor.org/info/rfc8554

12 – A. Huelsing, D. Butin, S. Gazdag, J. Rijneveld, J., A. Mohaisen, "XMSS: eXtended Merkle Signature Scheme", RFC 8391, DOI 10.17487/RFC8391, May 2018, https://www.rfc-editor.org/info/rfc8391

13 - B. Kaliski, "Securing the DNS in a Post-Quantum World: Hash-Based Signatures and Synthesized Zone Signing Keys, January 2021, https://blog.verisign.com/security/securing-the-dns-in-a-post-quantum-world-hash-based-signatures-and-synthesized-zone-signing-keys/

14 - A. Fregly, R. van Rijswijk-Deij, “Stateful Hash-Based Signatures for DNSSEC”, March 2022, https://www.ietf.org/archive/id/draft-afrvrd-dnsop-stateful-hbs-for-dnssec-00.txt

15 – H. Orman, “Internet Security and Quantum Computing”, December 2021, https://eprint.iacr.org/2021/1637.pdf

powered by

VERISIGN®